CURRENT APPROACHES IN MODERN CRYPTOLOGY

Mircea Andraşiu[1]

1. Abstract

This work proposes a brief analysis of the different types of current approaches to modern cryptology in present days. Due to increased development of communications and IT technologies, the field of cryptography practical approaches exceeded your government / military / intelligence / bank, eventually passing the civil environment and / or private. This process has soared in recent years and the requirements of market economy have forced a trend towards standardization of the theory and practice in cryptology. From there follows a rapid dissemination, sometimes without authorized assessment any official post by a wide range of users, including the private sector.

This purposes as stated above, we try an analysis of current patterns of cryptology approach to find action ways for national authorized entities to follow in the near future to synchronize efforts made in the same field of other countries and / or alliances or international organizations.

Finally, it should be noted that we considered only the approach of the different types of entities of the cryptologic phenomenon, without regard to side - the scientific approach, which may be subject to other works.

2. Introduction

In the international cryptologic environment is almost unanimously recognized that the starting point of modern cryptography is marked with the reference work of the two rebel, Whitfield Diffie and Martin E. Hellman, New Directions in Cryptology respectively, IEEE Transactions on Information Theory, 1976.

Underlying mathematical models and strong development of communications and IT technologies in the last 30 years have dramatically changed the interests and typology of approaches in cryptology and for cryptology.

Thus, modern cryptology brought standardization where it is known that in general there should be only imagination and inventiveness. Then, for the first time in long history of this science, progress in this area is done as public projects through a large collaboration between the academic - theoretical and technological aspects - practical.

---

[1] Mircea Andraşiu, CertSign

Thus, instead of a "production" held in very circumscribed areas public competitions take place, with the use of all the top results in key areas of theoretical and practical research.

Without having exhausted the subject, I think it is appropriate to mention the cryptology importance at the strategic level, meaning that this subject became the subject of working both at government levels and for large entities / state alliances worldwide, with all two-way implications resulting from here.

Recently occurs a new "atomization" approach, instead of global one, in which household cryptographic products are transformed into their simplest elements, elementary - atoms, primitive- which is studied individually in the best performance, then recomposed to obtain the cryptographic products of the highest scientific level.

We further detail each of the issues raised previously.

A. The 'atomic' approach (the types of primitive projects)

Let us briefly consider three types of projects, two on EU funding (EU) and one Japanese. They are Ness and e-Stream CRYPTREC respectively.

A1. NESSIE Project **(N**ew **E**uropean **S**chemes for **S**ignature, **I**ntegrity, and **E**ncryption) was started on January 1, 2000 with a deployment period of 3 years.

This project was financed by EU funds under the Information Societies Technology (IST) Program of the European Commission. There attended 7 universities and research centers in 6 countries.

In terms of the progress of activities, the project began with the launch of an application to participate in a public competition for cryptographic algorithms, with the deadline for submitting applications for evaluation on September 29, 2000.

Cryptographic algorithms had to meet certain requirements both cryptographic and for physical performance and implementation requirements at the technological level existing at the time. By the time stipulated above, there were 40 applications for assessment of cryptographic algorithms.

They covered a wide spectrum from symmetric algorithm type or block stream to digital signature schemes and public key encryption schemes. Remarkable fact, on this occasion it was requested assessment methodologies for cryptographic

algorithm in order to enhance trust and establish a common platform for their evaluation.

Compared with previous similar projects CRYPTREC AES the intention of this project was to propose to the government standards for cryptographic algorithms. For example, the algorithms for digital signature and hash functions have been included in the EESS standard documents specifying the encryption algorithms approved by the European Directive on electronic signature.

The project included several phases of partial evaluation as:

• First evaluation: September 2001, Egham, England, 24 algorithms are selected from 40 algorithms;

• Second evaluation: November 2002, Munich, Germany - Workshop, 12 algorithms remain, 5 proposed by the organizers directly;

• Final analysis: in February, 2003, Lund, Sweden, 17 algorithms were accepted.

Following the evaluation process have been accepted a number of primitive - atoms - elements, and final results are presented in the following table.

As you can see, some primitive -"atoms"- vital component of building a cryptosystem have no supported products, which may be an open question for the future. The same situation may also occur in cases with more representatives, where the comparative analysis can generate progress in the field.

No.	**Primitive**	**1. Supported products**
1	**Block Ciphers**	- **MISTY1 (**Japan), **Camellia (**Japan), **SHACAL-2(**France), **AES(USA FIPS 197) (Rijndael).**
2	**Synchronous stream ciphers**	
3	**Stream ciphers with autosychronization**	

4	**(MAC) Message authentication codes (MAC)**	- **Two-Track-MAC (Belgium, Germany);** **- UMAC: (USA, Israel);** **- CBC-MAC * (ISO / IEC 9797-1);** **- HMAC * (ISO / IEC 9797-1);** **- SHA-256 *, - * and 384 - 512 * (U.S. FIPS 180-2).**
5	**Collision-resistant hash function**	
6	**One-way hash function**	**Whirlpool (Brazil, Belgium);**
7	**Families of pseudo-random functions**	
8	**Asymmetric Encryption**	- **ACE Encrypt: (Switzerland);** **- PSEC-KEM (Japan);** **- RSA-KEM * (draft ISO / IEC 18033-2).**
9	**Asymmetric digital signature**	- **ECDSA: (U.S.,** Canada); **- RSA-PSS (USA);** **- SFLASH: (France).**
10	**Asymmetric identification schemes**	- **GPS: (France).**

A2. The E-Stream is also an EU project (IST respectively), that the IST was released in 2004 and its three phases lasted until 2008. There were 5 work - annual shops in Belgium, Denmark, from New Belgium, Germany and Switzerland and the goal was to obtain stream cipher type primitives. Portfolio's - STREAM completed in April 2008, revised in September that year, including two profiles:

- Profile 1 (Soft): HC-128 F, Rabbit Grain, Salsa 20/12 , SOSEMANUK ; 20/12;
- Profile 2 (Hard): FCSR-H v2, Grain v1, MICKEY v2 , Trivium .

Note that the project included an assessment activity, according to predetermined criteria. Results of the evaluation are known, but additional data on the performance of each product and some data about evaluation are considered confidentially. It can be requested directly from IST and are available only under the legal provisions in force at EU level - respectively IST.

A3.CRYPTREC project is considered as the main argument of the great progress made by Japanese business, scientific and technological environment in cryptography field. It is part of the official policy of Japan to build e - governance.

It was released in 2001, with the following types of primitives in attention:

- (1) Asymmetric algorithm for confidentiality, authenticity, digital signature and key exchange;
- (2) Symmetric algorithms: cipher block (64 and 128 bits) and stream cipher;
- (3) Hash functions (128 bits and more);
- (4) Pseudo number generator - Random.

There were originally proposed 31 algorithms - candidates, who after repeated selections formed the official list for the Japanese e-government.

For the legitimacy of using these algorithms - cryptographic algorithms in general - the government at that time promulgated in February 28, 2003 the directive " Policy for the use of ciphers to be used for procurement of each agency information system", which stipulates the obligation of all government agencies to use only algorithms from the abovementioned list.

B. The “Standards” approach

Technical public (civil) environment - and even within its academic environment - has been and will be at the forefront in terms of standardization in IT, with direct implications in cryptology

IT market requirements and security needs of commercial firms that have interests, but also obligations regarding protection of confidential business data or have led to the definition and acceptance of standards in the field of cryptology.

From this perspective we meet at least three levels of standardization, as follows:

- International: ISO, IEC, ITU;
- National: ANSI, BSI, NIST;
- Organizational: 3GPP, ETSI, IEEE, IETF, SECG, PKCS's;

For documentation, we briefly consider the ISO standards, the most internationally recognized.

The Chapter reserved to cryptology includes the following branches:

B1.1. Selected PKCS Standards

B1.2. The major standards for hash functions

B1.3. Standardized CBC-MAC Algorithms

B1.4. ISO / IEC 9797-1 MAC Algorithms

B1.5. Unilaterally Authentication Protocols Using Symmetric Crypto

B1.6. Mutual Authentication Protocols Using Symmetric Crypto

B1.7. TTP-Aided Mutual Authentication Protocols

B1.8. Unilaterally Auth. Protocols Using Asymmetric Crypto

B1.9. Mutual Authentication Protocols Using Asymmetric Crypto

B1.10. Manual Authentication Protocols

Note that some of the ISO standards are classified. For documentation we detail the preparation for one of the branches. For example, hash functions, sub - related sub-standards are:

- ISO / IEC 10118-1 (General information about hash functions);
- ISO / IEC 10118-2 (Hash functions using an n-bit block cipher);
- ISO / IEC 10118-3 (dedicated hash functions);
- ISO / IEC 10118-4 (Hash functions using modular arithmetic);
- NIST FIPS Pub. 180-2 (the SHA family of dedicated hash functions);
- IETF RFC 1319 (MD2);
- IETF RFC 1320 (MD4);
- IETF RFC 1321 (MD5);
- IETF RFC 3174 (SHA-1).

As noted, from those suggested above, there is a relentless concern for standardization in the trading environment, which at first sight conflicts with the

fact that the field of cryptology originally wanted *a science of secret writing* which only a limited group of initiated had access.

The authors' point of view is that the business environment will be increasingly more to say in the development field of cryptology and its standardization and the manner of approach will penetrate increasingly more in the government / military area.

C. The "Strategic" approach

If we talk about strategic approaches to cryptology, it should be noted that there are already major concerns in this regard on various international levels. Thus we should note the following approach to international organizations or arrangements:

- NATO;
- EU;
- OECD;
- WASSENAAR, etc…

Next we briefly review approaches to cryptography by the above organizations.

C1. NATO

In terms of production, are accepted only member countries products.

The certification is strictly done by the NATO specialized structure, or by national authorities having responsibilities in that field and which are recognized-accredited by the specialized structure of NATO.

The distribution and its management are the responsibility of national distribution authority from member countries.

C2. EU - European Union's approach on the field of cryptology is based on two principles, namely:

1. National production (EU countries);
2. Assessment by appropriately qualified authority (AQUA).

Consequently, cryptographic products designed to protect the privacy of EU classified information evaluation and approval by the appropriate qualified authority (AQUA) of a EU Member State must be supplemented by:

- The requirement that the products are designed and produced in a Member State of the Union;

- A further evaluation conducted by an appropriately qualified authority of a EU member state, which is not involved in the design or production.

Currently Romania has cryptographic-evaluation testing laboratories accredited by the national industry, which will be entered in the EU as AQUA authority following the accreditation procedures in this regard to be carried out soon.

C3. OECD - Organization of highly developed countries stands at the highest strategic level cryptographic work and principles (below) are general and can be successfully accepted and nationally.

These general principles promoted by the OECD in cryptography are:

1. Trust in cryptographic methods

Cryptographic methods should be trusted to provide certainty to users of computer systems and communications.

2. Choice of cryptographic methods

Users should have freedom to choose any cryptographic method which is subject to the laws in force.

3. Development of cryptographic methods required by the market

Cryptographic methods should be developed according to needs, demands and responsibilities of individuals, organizations, governments clearly in tune with market economy laws.

4. Standardization of cryptographic

Technical criteria and protocols for cryptographic methods must be developed and promulgated at national and international standards.

5. Protection privacy and personal data.

Be observed in the cryptographic policies and in the implementation and use of cryptographic methods, the fundamental rights of individuals, including those relating to confidentiality of communications and protection of personal data.

6. Legal access

National cryptographic policies may allow lawful access to the unencrypted data or to the cryptographic keys fore encrypted text.

These policies should fully respect the other principles covered in the guidelines.

7. Liability

Established by contract or by law, must be stated clearly, the liability of individuals or entities that offer cryptographic services or hold or access cryptographic keys.

8. International cooperation

Governments must cooperate to effectively coordinate the cryptographic policies. In this context they should remove or avoid creating, in the name of cryptographic policy, unjustified trade restrictions.

C4. Wassenaar Arrangement - this international agreement has a chapter on cryptography.

States participating in the Wassenaar Arrangement are: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, **Romania,** Russian Federation, Slovakia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and the United States.

Part relating to cryptography is given in Chapter five: "Telecommunications and Information Security", Part Two: "Information Security "in the document the EU Regulation (EC) no. 394 / 2006 of 27 February 2006 amending Regulation (EC) no. 1334 / 2000 establishing a Community system of export control of dual-use goods and technologies.

4. Conclusions

On careful analysis, the book is addressed not only to the specialists in cryptology, but may rather address to the leaders from different areas of activity where, in one way or another, are used results and cryptologic products.

First, a first conclusion is about the scale of the types of approaches to cryptography and to the national and international entities involved in this activity.

This raises a number of national responsibilities, which in turn naturally leads to the need for a uniform approach to various aspects of cryptography, on the national level.

There is appearance, not insignificant, on the acceptance and use of standards in cryptology, as they are already promoted and accepted by other countries, organizations and alliances.

Finally from the analysis of projects presented - and not only them - clearly result the need for national involvement - decision-making, scientific and technological level - based on capabilities and available resources at a time.

Based on these can be located precisely those niches - primitive - atoms that are available, so we still contested or even those that have already been accepted in order to ensure increased performance and their characteristics, by the national scientific and technological contribution.

5. References

[1]. Alexander W. Dent, Chris J. Alexander W. Dent, Chris J. Mitchel, User's guide to Cryptography Mitchell, User's Guide to Cryptography and Standards.and Standards. Artech House, 2005, Artech House, 2005,
[2] Bruce Schneier : Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C – 1996, [2] Bruce Schneier: Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C - 1996
[3]. ISO standards: http://www.iso.ch/ ISO standards: http://www.iso.ch/
[4]. IEC standards: http://www.iec.ch/ IEC standards: http://www.iec.ch/
[5]. ITU standards: http://www.itu.int/ITU-T/ ITU Standards: http://www.itu.int/ITU-T/
[6]. ANSI standards: http://webstore.ansi.org/ ANSI standards: http://webstore.ansi.org/
[7]. BSI standards: http://www.bsi-global.com/ BSI standards: http://www.bsi-global.com/
[8]. NIST standards: http://www.nist.gov/ , http://www.csrc.nist.gov/ NIST standards: http://www.nist.gov/, http://www.csrc.nist.gov/

[9]. 3GPP standards: http://www.3gpp.org/ 3GPP standards: http://www.3gpp.org/
[10]. ETSI standards: http://www.etsi.org/ ETSI standards: http://www.etsi.org/
[11]. IEEE standards: http://standards.ieee.org/ IEEE standards:
http://standards.ieee.org/
[12]. IETF standards: http://www.ietf.org/ IETF standards: http://www.ietf.org/
[13]. SECG standards: http://www.secg.org/ SECG standards:
http://www.secg.org/
[14]. PKCS standards: PKCS standards:
http://www.rsasecurity.com/rsalabs/pkcs/index.html
http://www.rsasecurity.com/rsalabs/pkcs/index.html
[15]. NESSIE evaluation project: http://www.cryptonessie.org/ NESS evaluation
project: http://www.cryptonessie.org/
[16]. ECRYPT evaluation project: http://www.ecrypt.eu.org/ ECRYPT evaluation
project: http://www.ecrypt.eu.org/
[17]. CRYPTREC evaluation project: CRYPTREC evaluation project:
http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html e /
http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html e /